Atty. Dkt. No. 30003039-2 #4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Keith Alexander HARRISON et al.

Title: IMPROVEMENTS IN AND RELATING TO METHODS OF COMMUNICATION

Appl. No.: Unassigned

Filing Date: December 21, 2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

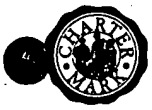
Great Britain Patent Application
No. 0031420.3 filed 12/22/2000.

Respectfully submitted,

Date: December 21, 2001

By _____

William T. Ellis
Attorney for Applicant
Registration No. 26,874



The Patent Office
COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

#4

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

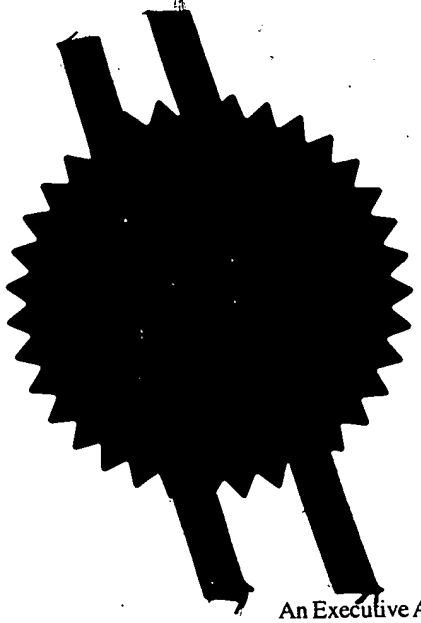
CERTIFIED COPY OF PRIORITY DOCUMENT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

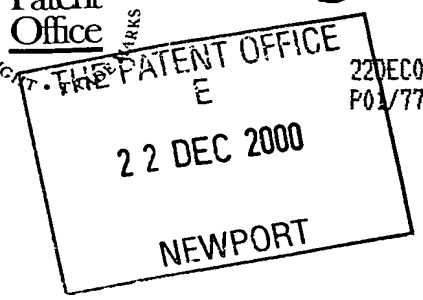


Signed J Evans.

Dated 6 February 2001

Patents Form 1/77

Patents Act 1977
(Rule 16)



22DEC00 E593783-1 D01463
P01/7700 0.00-0031420.3

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 30003039 GB

2. Patent application number
(The Patent Office will fill in this part) — **0031420.3** — 22 DEC 2000

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number *(if you know it)* 4965880004

Delaware, USA

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention — Improvements in and relating to methods of communication

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Richard A Lawrence
Hewlett-Packard Ltd, IP Section
Filton Road
Stoke Gifford
Bristol BS34 8QZ

Patents ADP number *(if you know it)* 7563083001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	12
Claim(s)	6
Abstract	1
Drawing(s)	1+1

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1 /
Request for preliminary examination and search *(Patents Form 9/77)*	1 /
Request for substantive examination *(Patents Form 10/77)*	-
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature Date

Richard A Lawrence 21/12/2000

12. Name and daytime telephone number of person to contact in the United Kingdom

Julie Miles Tel: 0117-312-8026

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

IMPROVEMENTS IN AND RELATING TO METHODS OF COMMUNICATION

The present invention relates to methods of communication and to composite credentials.

In communication across a distributed electronic network such as the internet, particularly (but not exclusively) in a business to business communication, there may be many separate business to business communications required for a single action or transaction.

Figure 1 of the drawings that follow illustrates such a known communication method and system. In Figure 1 there is shown a first party 2 in communication with a set 4 of other enterprises comprising a second party 6, third party 8, fourth party 10, fifth party 12 and sixth party 14, respectively some of which are in communication with each other as indicated by the arrows in Figure 1. Communication between the first party 2 and the set of other enterprises 4 is across the internet (indicated schematically at 16). Communication between the second to sixth parties 6-14, respectively may be across the internet, but could also be across a wide area network (WAN) or local area network (LAN). Typically, each party will be an enterprise such as a business.

If the first party 2 wishes to communicate reliably with the second party 6, for instance to carry out a financial transaction it is necessary for first party 2 to provide a credential 18 to the second party 6.

A credential is a data structure provided to the bearer for a purpose with some acknowledged way to verify the bearers right to use the credential.

In the digital environment a credential will generally be an electronic document which has a defined structure known to all involved parties. Credentials are issued by an authority (sometimes referred to as a trusted source). Typically the credential has additional data (ie a digital signature) that "ties" the document content to the issuer.

Typically a credential will comprise information concerning the bearer (perhaps identity details or financial records) and will be digitally signed by a trusted source. Verification is achieved by decryption of the digital signature. Generally a credential performs the functions of authentication and authorisation.

The purpose of the credential is to identify the user and/or to validate a transaction between parties, which transaction may be the transfer of information which needs to be validated. However, for the second party 6 to complete the transaction it needs (in this example) to communicate with the third and fourth parties 8, 10 respectively. The third and fourth parties 8, 10 respectively each communicate separately with fifth party 12, which in turn communicates with sixth party 14. Each party 6-14 may require a different credential from first party 2 to validate its part of the transaction. In this example, third party 8 requires a second credential 20 from first party 2 and fifth party 12 requires a third credential 22 from first party 2. Thus, third party 8 and fifth party 12 need to communicate separately with a first

party 2 to obtain the second and third credentials 20, 22 respectively. This, therefore, is a multi-layer communication. First party 2 will not necessarily be aware of the need at the beginning of the transaction for the third and fifth parties 8, 12 respectively to be involved so extra validation and credential transfer may be required.

To undertake such a transaction, data continuously has to be sent back and forth between the involved parties. This increases the possibility of an external attack. To minimise the risk of an attack, data has to be protected and verified by each party of a transaction at each step, which reduces the overall performance.

Moreover, such a method of communication requires many separate communications between the parties. Specifically, the first party is involved in several communications which is undesirable.

It is an aim of preferred embodiments of the present invention to improve performance in such communication environments.

According to the present invention in a first aspect, there is provided a method of communication, the method comprising the steps of a first party communicating to a second party a composite credential across a distributed electronic network which composite credential comprises a plurality of credentials.

A credential for the purpose of the present invention is a data structure provided to the bearer for a purpose with

some acknowledged way to verify the bearers right to use the credential.

Suitably, second party communicates at least part of the composite credential to a third party. The second party may modify the received composite credential before communicating it to the third party. The modification may be by addition to and/or removal from the composite credential. Suitably, the second party communicates the received composite credential to the third party.

According to the present invention in a second aspect, there is provided a composite credential for communication of credentials across a distributed electronic network, the composite credential comprising a plurality of credentials.

The use of such a composite credential can reduce the number of communications required in a multi-layer transaction.

Suitably, at least one credential in the composite credential is obfuscated. Obfuscation is a process whereby data is rendered not easily intelligible to an unauthorised recipient. Generally, obfuscation will be by encryption but may also be by data compression or in other way. Suitably, a plurality of credentials in the composite credential is obfuscated. Suitably, all credentials are obfuscated within the composite credential. Suitably, different obfuscation is used for at least two credentials in the composite credential. Suitably, different obfuscation is used for each

obfuscated credential in the composite credential. Suitably, the obfuscation comprises asymmetric encryption.

In the above method of communication, suitably the first party communicates to the second party the composite credential, which composite credential is at least partly obfuscated, and the second party de-obfuscates a relevant credential.

Suitably, the composite credential comprises a first credential and a second credential in which the second credential is enveloped by the first credential. Such a composite credential can be used to dictate the order in which the credentials within the composite credential can/must be read and therefore a workflow.

In a method of communication, suitably a first party communicates to a second party a composite credential according to the preceding paragraph, which composite credential is de-obfuscated by the second party thereby to obtain the first credential and a partly de-obfuscated second credential, which party de-obfuscated second credential is communicated by the second party to a third party. Suitably, the third party de-obfuscates the partly de-obfuscated second credential.

Suitably, the composite credential is obfuscated. Suitably, the obfuscation comprises an asymmetric encryption.

Suitably, in a composite credential in which a plurality of credentials is variably obfuscated, a second party de-obfuscates at least one credential and communicates to a

third party at least one obfuscated credential from the composite credential. In this way credentials can be sent to be readable only by the party or parties for which they are intended.

Suitably, at least one credential is digitally signed. Suitably, a plurality of credentials is digitally signed. Suitably, all credentials in the composite credential are digitally signed. Suitably, the composite credential is digitally signed.

Suitably, the distributed electronic network is the internet.

The composite credential of the first aspect of the invention may be according to the second aspect of the invention.

The present invention will now be described, by way of example only, with reference to the drawings that follow; in which:

Figure 1 is a schematic functional illustration of a method of communication as required by the prior art.

Figure 2 is a schematic functional illustration of a method of communication according to the present invention.

Referring to Figure 2 of the drawings that follow, there is shown a first enterprise 30 in digital communication with a second enterprise 32, which second enterprise is in digital communication with third and fourth enterprises

34, 36 respectively, each of which in turn is in communication with a fourth enterprise 38, which is in communication with a fifth enterprise 40. The second to sixth parties 32-40 respectively form a set of enterprises 42 required to complete a communication between first and second parties 2, 4 respectively.

Communication between first party 2 and second party 4 is across the internet (though it need not be), indicated schematically at 44.

To complete the communication, second party 32 requires a first credential 46 from first party 30, third party 34 requires a second credential 48 from first party 30 and fifth party 38 requires a third credential 50 from first party 30 (as in the prior art example referred to above in relation to Figure 1).

The first, second and third credentials 46-50 respectively are stored with a fourth credential 52 in a composite credential 54. In this embodiment, the composite credential 54 comprises a data file (eg a HTML form, an XML file, a WORD (trade mark) file or even just plain ASCII text) containing the first, second and third credentials 46-50 respectively. The composite credential 54 is digitally signed by the first party 30. Digital signing allows for modifications to the data to be detected and identifies who the signer was.

The composite credential 54 is sent by the first party 30 via the internet to second party 32, which extracts the required first credential 46 from the composite credential 54 and passes the composite credential 54 to third and

fourth parties 34, 36 respectively along with any other information necessary for their (the third and fourth parties 34, 36 respectively), part of the communication.

Third party 34 verifies the composite credential 54 by decrypting the digital signature and extracts second credential 48 from the composite credential 54, uses second credential 48 as required, and passes the composite credential 54 along with any other information required to fifth party 38. Fourth party 36 does not require a credential and so does not need to examine the composite credential 54. Fourth party 36 passes on the required information and the composite credential 54 to fifth party 38. Fifth party 38 extracts third credential 50 from composite credential 54 and uses it as required together with the other information with which it has been supplied.

It is noted that third and fifth parties 34, 38 respectively obtain the second and third credentials 48, 50 respectively of the first party 30 from composite credential 54 without the need for them to communicate directly with the first party 30. Accordingly, the number of communication operations required to complete the communication is reduced and, performance is increased.

The fourth credential 52 is not required as part of this communication but can (with other credentials) be included in composite credential 54 as it may be of use in other communication transactions.

Thus, the first party 30 can have a single composite credential 54 for use in a plurality of communication

transactions, other parties choosing the credentials they want or need from the composite credential 54 even if not all of the credentials are required for the particular communication transaction. Further the first party 30 may have a plurality of discrete composite credentials each containing a different combination of (not necessarily the same) credentials.

One or more credentials in the composite credential 54 may be obfuscated. Each credential 46-52 may be obfuscated using a different form of obfuscation. Accordingly only certain of the second to sixth parties may have the knowledge (as required) to de-obfuscate the credential(s) they require. Obfuscation may be by symmetric (eg Digital Encryption Standard (DES) or Internation Data Encryption Algorithm (IDEA)) or asymmetric (eg public/secret key) encryption. An alternative forms of obfuscation is data compression for instance by using WINZIP (trade mark). Obfuscation of the credentials 46-52 enhances security. Thus, while obfuscation preferably involves encryption, it need not.

Each party upon receipt of composite credential 54 may pass on (i) the original composite credential 54, (ii) a version excluding the credential the transmitting party has used (this requires knowledge on the part of the transmitting party that the receiving party and any subsequent using party will not need the excluded credential), (iii) a version with one or more previously obfuscated credentials de-obfuscated (which reduces the security of the method, but also reduces processing requirement for subsequent parties so may be appropriate, for instance, where the subsequent parties are within the

same organisation as the transmitting party) or (iv) a version with additional data added. If a modified composite credential is transmitted, the modifier will digitally sign the modified data.

Further, de-obfuscation of a credential may be dependent on de-obfuscation of a preceding credential. For instance, by way of example, a first credential 46 is obfuscated using a first key known to the second party 32 only. The second credential 48 is obfuscated by a second key, which second key requires knowledge of the first key. For instance, a session key for the second credential may be embedded in the obfuscated first credential. Even when de-obfuscated from the first credential, the session key for the second credential may remain obfuscated, to be de-obfuscated by the third party.

Only the third party 34 has the knowledge to read the obfuscated second credential 48, but the knowledge it has is only sufficient if it has received the de-obfuscated first credential 46. Once it has done so it can de-obfuscate the second credential and use it as required. This enveloping of credentials can be used as many times as desired to control the order in which parties subsequent to the first party 30 can access the credentials.

The composite credential 54 will usually be digitally signed to validate it as having been signed by a recognised party and enable the recipient to establish whether it has been modified at all. The composite credential 54 may be digitally signed by each party before transmission to validate the source and content thereof.

This can also be used to maintain an audit trail for the composite credential 54. However, composite credentials (and credentials within the composite credentials) that are not digitally signed also fall within the scope of the present invention.

The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

The invention is not restricted to the details of the foregoing embodiment(s). The invention extend to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel

combination, of the steps of any method or process so disclosed.

Claims

1. A method of communication, the method comprising the steps of a first party communicating to a second party a composite credential across a distributed electronic network which composite credential comprises a plurality of credentials.

2. A method of communication according to claim 1, in which second party communicates at least part of the composite credential to a third party.

3. A method of communication according to claim 2, in which the second party modifies the received composite credential before communicating it to the third party.

4. A method of communication according to claim 2, in which the second party communicates the received composite credential to the third party.

5. A method of communication according to any preceding claim, in which at least one credential in the composite credential is obfuscated.

6. A method of communication according to claim 5, in which a plurality of credentials in the composite credential is obfuscated.

7. A method of communication according to claim 5, in which all credentials are obfuscated within the composite credential.

8. A communication method according to claim 6 or claim 7, in which different obfuscation is used for at least two credentials in the composite credential.

9. A method of communication according to claim 7 or claim 8, in which different obfuscation is used for each obfuscated credential in the composite credential.

10. A method of communication according to any one of claims 5 to 9, in which the obfuscation comprises asymmetric encryption.

11. A method of communication according to claim 8 or claim 9, in which in a composite credential in which a plurality of credentials is variably obfuscated, a second party de-obfuscates at least one credential and communicates to a third party at least one obfuscated credential from the composite credential.

12. A method of communication according to any preceding claim, in which the composite credential comprises a first credential and a second credential in which the second credential is enveloped by the first credential.

13. A method of communication according to any preceding claim, in which a first party communicates to a second party a composite credential according to claim 12, which composite credential is de-obfuscated by the second party thereby to obtain the first credential and a partly de-obfuscated second credential, which

party de-obfuscated second credential is communicated by the second party to a third party.

14. A method of communication according to claim 13, in which the third party de-obfuscates the partly de-obfuscated second credential.

15. A method of communication according to any one of claims 1 to 4, in which the composite credential is obfuscated.

16. A method of communication according to claim 15, in which the obfuscation comprises an asymmetric encryption.

17. A method of communication according to claim 15 or claim 16, in which the first party communicates to the second party the composite credential, which composite credential is at least partly obfuscated, and the second party de-obfuscates a relevant credential.

18. A method of communication according to any one of claims 1 to 4, in which at least one credential is digitally signed.

19. A method of communication according to claim 18, in which a plurality of credentials is digitally signed.

20. A method of communication according to claim 18, in which all credentials in the composite credential are digitally signed.

21. A method of communication according to any one of claims 1 to 4, in which the composite credential is digitally signed.

22. A method of communication according to any preceding claim, in which the distributed electronic network is the internet.

23. A composite credential for communication of credentials across a distributed electronic network, the composite credential comprising a plurality of credentials.

24. A composite credential according to claim 23, in which at least one credential in the composite credential is obfuscated.

25. A composite credential according to claim 24, in which a plurality of credentials in the composite credential is obfuscated.

26. A composite credential according to claim 24, in which all credentials are obfuscated within the composite credential.

27. A composite credential according to claim 25 or claim 26, in which different obfuscation is used for at least two credentials in the composite credential.

28. A composite credential according to claim 26, in which different obfuscation is used for each obfuscated credential in the composite credential.

29. A composite credential according to any one of claims 24 to 28, in which the obfuscation comprises asymmetric encryption.

30. A composite credential according to any preceding claim, in which the composite credential comprises a first credential and a second credential in which the second credential is enveloped by the first credential.

31. A composite credential according to claim 23, in which the composite credential is obfuscated.

32. A composite credential according to claim 31, in which the obfuscation comprises an asymmetric encryption.

33. A composite credential according to claim 23, in which at least one credential is digitally signed.

34. A composite credential according to claim 33, in which a plurality of credentials is digitally signed.

35. A composite credential according to claim 33, in which all credentials in the composite credential are digitally signed.

36. A composite credential according to claim 23, in which the composite credential is digitally signed.

37. A method of communication substantially as described herein, with reference to Figure 2 of the drawings that follow.

38. A composite credential substantially as described herein, with reference to Figure 2 of the drawings that follow.

ABSTRACT

IMPROVEMENTS IN AND RELATING TO METHODS OF COMMUNICATION

The present invention provides a method of communication, the method comprising the steps of a first party (30) communicating to a second party (32) a composite credential (54) across a distributed electronic network (44) which composite credential (54) comprises a plurality of credentials (46-52). A corresponding composite credential is also disclosed.

Figure 2

FIGURE 1

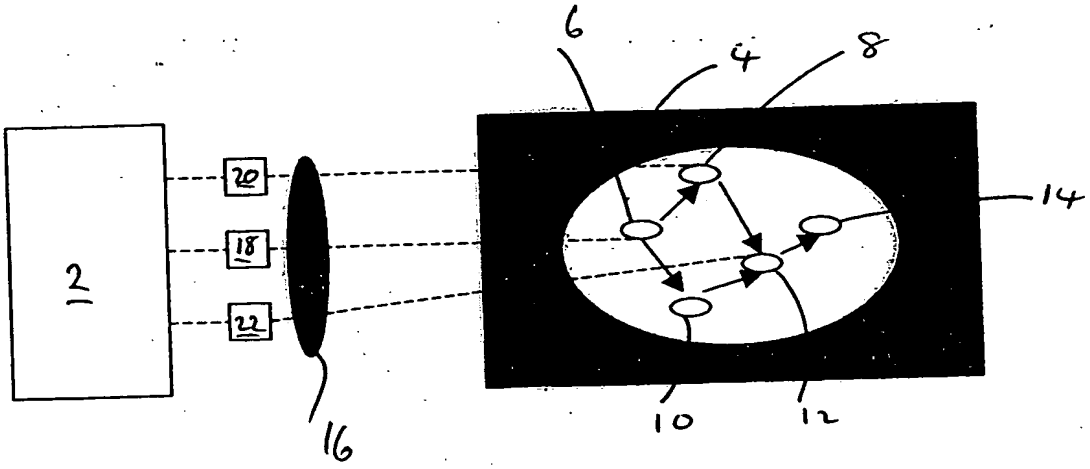
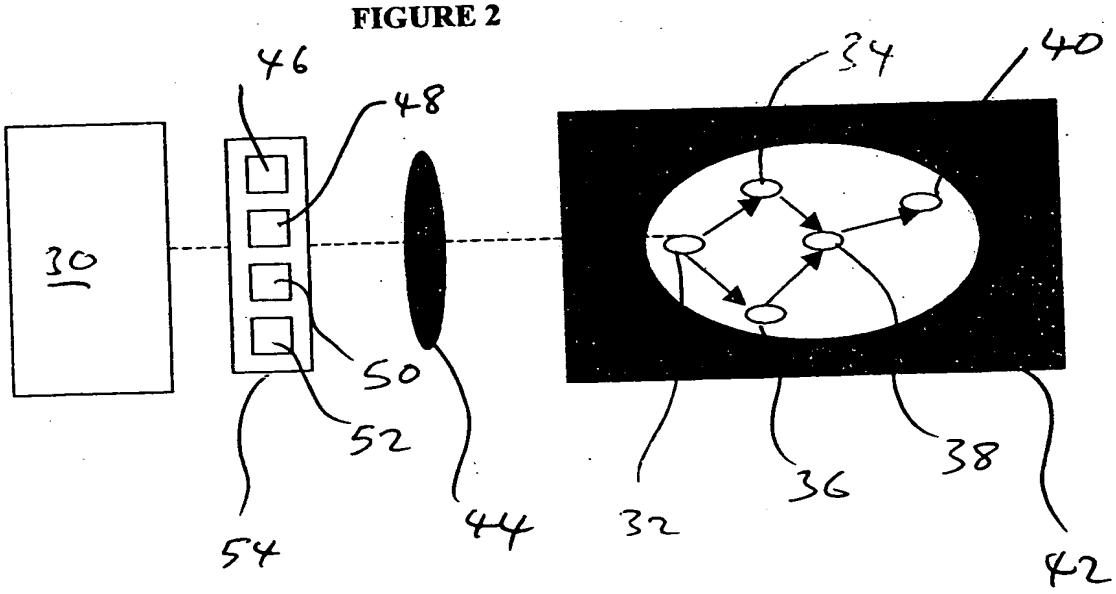


FIGURE 2



THIS PAGE BLANK (USPTO)

30003039-2 WTE Harrison

Foley & Lardner
3000 K Street, N. W. Suite 500
Box 25696
Washington, D. C. 20007-8696